




## City of Riverside Administrative Manual

---

Effective Date: 01/2009  
Review Date: 07/2012  
Prepared by: City Manager/Finance

Approved:

  
\_\_\_\_\_  
Department  
City Manager

### SUBJECT:

### Credit Card Acceptance Policy

### PURPOSE:

This policy establishes standards for the acceptance and processing of credit card payments in City departments and maintaining the security of confidential credit card data. The federal Fair and Accurate Credit Transactions (FACT) Act of 2003 requires creditors (defined in the Act to include *municipally-owned public utility companies or other public entities that extend credit*) to implement reasonable policies and procedures for detecting, preventing and mitigating identity theft. This policy will supplement the City's Identity Theft Prevention Program required by the FACT Act to be implemented by May 2009.

Compliance with this policy will:

- Provide reasonable assurance that all credit card transactions are properly authorized, timely settled, and accurately and completely recorded;
- Monitor for errors, both unintentional and intentional, including fraud; and
- Protect the security, confidentiality and integrity of cardholder information.

This policy is further intended to ensure compliance with Payment Card Industry (PCI) Standards, as required by Visa, Mastercard, American Express and Discover. Failure to comply with PCI industry standards may result in fines and/or revocation of credit card acceptance.

### POLICY:

#### **Authorized Departments**

As of the date of this policy, the following departments are authorized to accept credit card transactions:

- |                        |                                |
|------------------------|--------------------------------|
| • Development          | • Parks, Rec. & Community Svc. |
| • City Manager-Finance | • Police                       |
| • Fire                 | • Public Utilities             |
| • Library              | • Public Works                 |

Departments accepting credit card payments must comply with credit card provider regulations, including the acceptance of credit cards for all transactions types and dollar amounts.

#### **Transaction Control Requirements**

The City accepts Visa, Mastercard, American Express and Discover credit cards as a form of payment of amounts due to the City. Debit cards with Visa or MasterCard logos are also accepted and processed as credit cards. The City currently accepts transactions through point-of-sale, telephone, internet and mail transactions. Each transaction type requires a unique set of processes to ensure the accurate processing and recording of transactions and guard against erroneous or fraudulent transactions.

### Point of Sale Transactions

1. Credit card machines and manual imprinters are to be secured and inaccessible to the public. However, a customer's credit card should be visible to the customer at all times during the transaction.
2. Prior to swiping the credit card:
  - a. Ensure that the credit card expiration date has not passed. Expired credit cards must not be accepted for payment.
  - b. Compare the name on the credit card to the cardholder's photo identification. If the names do not match, the credit card must not be accepted for payment.
3. Ensure that the amount charged to the card matches the transaction. No refunds or credits may be issued in conjunction with the payment.
4. A signature must be obtained on the credit card payment slip and compared to the signed credit card or the credit card owner's photo identification. In the event of unmatched signatures, the credit card transaction must be voided and the credit card returned to the customer.
5. If the credit card's magnetic strip cannot be read, the card number should be keyed into the credit card terminal. To reduce the risk of access to confidential credit card data, manual imprints of the card should not be made.
6. If the authorization network (via the credit card machine or the Address Verification Service) sends a "decline" or "no match" response, the credit card must not be accepted.
7. In all circumstances of declined or unaccepted transactions, return the credit card to the customer and offer to accept another method of payment. Customers disputing the decline or non-acceptance of the credit card should be referred to their bank.

### Internet Transactions

1. The website must include fraud prevention measures such as Address Verification Services, Card Certification Value, Card Validation Code or other tools available through the bank or merchant service provider.

### Telephone and Mail Transactions

1. Key the credit card data including the card number, expiration date, street number and zip code into the credit card terminal. Failure to key in the address information results in higher credit card fees and increases the risk of fraud.
2. Ensure that the transaction documentation (e.g., remittance advice) contains the customer number, invoice number or other identifier. Do not accept credit card payments where either:
  - a. the credit card name does not match the customer name; or
  - b. the requirements of third-party transactions are met.

### Third-Party Transactions

The city will not accept third-party credit cards unless the one of the following criteria is met:

- ☐ The credit card name matches the identification of the individual presenting it; or
- ☐ The transaction documentation, such as the account or customer name, matches the name on the credit card.

### Third-party Payment Processors

No department will initiate credit card acceptance with a bank, merchant service provider or as a tie-in to third-party software without Finance division involvement and approval. Any computer system or internet-based payment processing will also require Information Technology review and approval to ensure the third party has adequate safeguards of confidential data in place, such as encrypted data transmission of card information.

The City currently contracts with third-party payment processors to accept credit card payments on behalf of the City. The applicable departments will work with the provider to ensure that a complete and accurate recording of transactions, fees and deposit of monies takes place in a timely manner. All third-party processors are expected to comply with Payment Card Industry standards.

### ***Settlement and Deposit of Credit Card Payments***

1. The daily receipt totals from point-of-sale credit card machines must be printed and used to settle transactions at the end of each business day.
2. The transaction history report from each credit card machine must be reconciled to the total credit card receipts.
3. The settlement batch, transaction history and reconciliation reports and supporting documentation must be remitted to the Treasury division on the following business day. Any items held overnight in the department must be secured to prevent against the theft of confidential customer data.
4. All credit card receipts and supporting documentation that are routed through interoffice mail must be secured in a locked currency bag.
5. Deposits are generally credited to the bank within 3 business days, depending upon the credit card type.

### ***Merchant Fees and Other Credit Card Charges***

Merchant fees for all point-of-sale transactions are netted on the City's bank statement against credit card receipts. Departments will be charged their proportional share of merchant fees.

Other credit card charges, such as charge-backs, disputed, and returned items are related to a specific transaction and will be referred to the applicable department for follow-up.

### ***Safeguarding of Confidential Data***

- Credit card records, including but not limited to, receipts, imprints, credit card numbers, expiration date, card type, bank information, etc. are exempt from public disclosure and shall not be disclosed by the City unless required via Court subpoena or in writing by the City Attorney.
- Any credit card documents not remitted to Treasury before the close of the business day must be secured to prevent against the theft of confidential customer data.
- If processing of credit card data is provided by a third party on the City's behalf, the service provider must be capable of maintaining the appropriate safeguards.
- Full credit card numbers must not be recorded, maintained or viewable in any computer systems.
- To the extent required by law, the City will notify credit card customers of any breach of security which has placed their confidential credit card information at risk.

### ***Payment Card Industry (PCI) Compliance***

The City will annually review and update PCI Self-Assessment Questionnaire (SAQ) D and Attestation of Compliance applicable to Validation Type 5 merchants. Merchants in Validation Type 5 process credit card transactions in a variety of manners, including stand-alone, dial-out terminals and internet payment systems.

The City will require that third-party processors accepting credit card payments on behalf of the City also complete the PCI SAQ applicable to their merchant validation type.

## PROCEDURE:

Responsibility	Action
City Department	<p data-bbox="553 331 1442 401">Follow City policy and procedures established for the processing and settlement of credit card payments.</p> <p data-bbox="553 415 1458 512">Provide adequate training of staff members to ensure compliance with the credit card policy and understanding of the related procedures and internal controls.</p> <p data-bbox="553 527 1305 560">Ensure that all credit card data is adequately safeguarded.</p> <p data-bbox="553 575 1463 672">Utilize locked currency bags when transporting credit card documentation via interoffice mail, and limit access to the currency bag keys to specific, authorized personnel.</p> <p data-bbox="553 686 1414 756">Perform reconciliation of payments to ensure accurate recording of transactions and deposits.</p> <p data-bbox="553 770 1471 840">Perform settlement procedures and remit required data to Treasury in a timely manner.</p> <p data-bbox="553 854 1458 921">Follow up immediately on charge-backs (disputed, returned or rejected items).</p> <p data-bbox="553 936 1474 1005">Report suspicious activity including possible fraud or theft to the Internal Audit division in a timely manner.</p>
Finance - Treasury	<p data-bbox="553 1045 1446 1142">Treasury will follow City procedures relating to bank statement review, credit card deposit verification and review of department data and recording of receipts.</p> <p data-bbox="553 1157 1479 1226">Record a monthly allocation of merchant fees to each department based upon the department's proportional share of credit card receipts.</p> <p data-bbox="553 1241 1305 1274">Ensure that all credit card data is adequately safeguarded.</p> <p data-bbox="553 1289 1474 1358">Report suspicious activity including possible fraud or theft to the Internal Audit division in a timely manner.</p> <p data-bbox="553 1373 1484 1442">Annually review and update the PCI Self-Assessment Questionnaire and Attestation of Compliance.</p> <p data-bbox="553 1442 1442 1539">Ensure that third-party processors accepting credit card payments on behalf of the City complete the PCI SAQ applicable to their merchant validation type.</p>
Information Technology	<p data-bbox="553 1562 1182 1596">Ensure adequate safeguarding of customer data.</p> <p data-bbox="553 1625 1451 1694">Ensure the adequacy of the control systems of electronic data of third-party vendors.</p>

Distribution: Regular